学校编码：10384　　分类号＿＿＿＿＿密级＿＿＿＿＿
学　　号：200028003　　UDC ＿＿＿＿＿＿＿＿＿＿＿＿

学　位　论　文

信息安全策略及其应用研究

徐晖

指 导 教 师：李翠华　教授
申请学位类别：硕　　士
专 业 名 称：计 算 机 应 用
论文提交日期：2003 年 5 月　日
论文答辩日期：2003 年　月　日
学位授予单位：厦 门 大 学
学位授予日期：2003 年　月　日

答辩委员会主席：＿＿＿＿＿＿＿＿
评　　阅　　人：＿＿＿＿＿＿＿＿

二〇〇三年五月

摘要

随着国际互联网逐步地深入到人们的日常工作、生活和学习中，信息安全问题越来越受到大家的关注，也成为了研究的热点问题。本文从公、私应用两个方面，对信息安全问题作了一定的研究和探讨。

隐私权问题是个人在上网时不得不面对的问题。社会生产方式的转变导致用户的个人信息成为商家猎取的目标，个人的隐私权无法得到保障。本文指出了商家侵犯隐私的深层原因，并给出了几种解决的方法。

电子政务是我国各政府机关一直以来积极推进的一项改革措施。其中，各种公文的安全传送一直是电子政务中急需解决的问题。在目前的情况下，各类公文只能够通过邮寄，速度很慢。而电子邮件系统虽然快速、便捷，但是互联网的开放性决定了它的不安全性，任何一个个人都可以拦截、篡改网上的信息。如何能够通过电子邮件来安全地传送各种公文是本文所要着重讨论的另一个问题。

在本文中，引入了一个混合式的加密体制，结合了单纯的公开密钥体制和传统密钥体制的优点，能够较好地完成对电子公文的加密，确保了级别较高的公文不被他人偷看。同时，以数字签名技术和单向散列函数为基础，可以对公文的完整性和发件方作确认。

本文共五章，第一章是概述部分。在第一章中，简单地介绍了有关信息安全的概念、基本特征以及信息安全涉及的内容，提出了本文的研究内容，总结了本文的主要贡献。

第二章是密码学的基础知识。介绍了密码学的专用术语，密码学的分类，对目前现有的数字签名算法和散列函数算法作了介绍，并分析了各种算法的优缺点及其发展前景。

第三章对网络中的隐私权保护问题作了阐述和分析，提出了几种解决方案。

第四章介绍了电子公文传送的实现方法，对每一个模块中的关键问题作了阐述，并与其它的电子公文传送系统相比较，分析了本系统的优点。

第五章是结束语，总结了本文的主要工作，并提出了下一步工作的设想。

关键词：数字签名，混合式加密，隐私权保护，电子公文传送

Abstract

With the development of computer technology and the explosion of Internet, information security becomes more and more important. In this paper, we do research on information security from public application and private application.

Privacy protection is the problem one has to face when he is surfing in Internet. Because of the shifting of social production form, customers's private information has become the salesman's target and the customer's privacy cann't be protected. In this paper, we point out the deep-seated reason and give the ways to resolve it.

Electronic government affair has always been a reformation that promoted actively by our government departments. Within it, the transporting of electronic document is the problem urgent to solve. At present, these document can only be transported through mail, while this way is time-taking and slow. Although e-mail is quick and convenient, it is quite insecurity because of the openness of Internet-------anyone can hold up or tamper with the information on Internet. How to transport the document through e-mail safely is another topic of this paper.

In this paper, a mixed encrypting/decrypting system combined the merit of public cipher system and traditional cipher system is introduced. It can encrypt the electronic document perfectly, insuring the document of high priority not to be stolen. At the same time, based on the digital signature and one-way hash function, it identifies the integrity of the document and the addresser.

This paper is divided into five chapters. The first chapter is summarization. It introduces the concept, basic characters and content of information security. Finally put forward the focus and contribution of this paper.

The second chapter is basic knowledge of cryptology-------introduces the technical terms and the classification of the cryptology, the arithmetic of the digital signature and the hash function in existence, finally analyses the merit and defect of these arithmetic and development foreground.

The third chapter put forward and analyze the problem of privacy protection in Internet, give the ways to resolve it.

The fourth chapter introduces the implementation of the system, explains the main problems of each modules, compares it with other electronic document transporting systems, and summarizes the merit of this system.

The fifth chapter is a conclusion.

Keywords: digital signature, mixed encrypting/decrypting, privacy protection
electronic document transporting

目 录

第一章 绪论 5
1．1信息安全的基本概念 5
1．2 信息安全的特征 5
1．3信息安全的基本内容 6
1．3．1实体安全 6
1．3．2运行安全 6
1．3．3信息资产安全 7
1．3．4人员安全 8
1．4本文的主要研究内容： 8
第二章 密码学的基础知识 9
2．1密码学的基本概念 9
2．2密码学的常用术语 9
2．3密码系统 10
2．3．1对称密钥密码系统 10
2．3．2公开密钥密码系统 12
2．4数字签名 15
2．4．1单向散列函数 17
2．4．2 数字签名算法 25
2．5 小结 29
第三章 互联网中隐私权的问题研究及其保护策略 31
3．1 简介 31
3．2 隐私权问题 32
3．3 侵害用户隐私的深层原因 33
3．4网上隐私保护技术 34
3．5 隐私保护发展趋势 36
3．6 小结 36
第四章 数字签名在电子公文传送中的应用与设计 37
4．1问题的分析 37
4．2算法的分析 37
4．3 问题的解决方法 39
4．4各功能模块的实现 40
4．4．1 MD5的实现 40

4．4．2 混合式的加密系统的实现 42
4．4．3 RSA 密码系统的实现..... 45
4．4．4 传送模块的实现..... 50
4.5 密钥的管理..... 54
4.6 本系统的优点及与其它系统的比较 55
4.7 小结 56
第五章　结束语 57
参考文献 59
研究生期间的研究成果 61
致　谢 63

第一章 绪论

互联网的发展日新月异，以极快的速度改变着人们的日常工作、学习和生活。但是，在其快速发展的过程中，信息安全问题已经引起了人们的极大关注。

1．1 信息安全的基本概念

信息安全问题是随着 Internet 的日益普及，信息网络技术的广泛应用而逐渐成为人们关注的热点。本身 Internet 具有的开放性、国际性和自由性增加了应用自由度，但是同时，对安全也提出了更高的要求，主要表现在[1]：

开放性的网络导致网络的技术是全开放的，任何一个个人、团体都可能获得，因而网络所面临的破坏和攻击可能是多方面的。国际性的网络还意味着网络受到的攻击不仅仅来自本地网络的用户，也可来自 Internet 上的任何一台机器，即网络安全面临的是一个国际化的挑战。

自由性意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络、自由地使用和发布各种类型的信息。用户只对自己的行为负责，而没有任何的法律限制。

目前，信息安全并没有一个公认的、统一的定义，国际、国内对信息安全的论述，可以分为两类：一类是指具体的信息技术系统的安全，另一类是指某一特定信息体系（如一个国家的银行信息系统、军事指挥系统等）的安全。

1．2 信息安全的特征

信息安全主要有以下四个基本特征：

一、完整性（integrity）

完整性即信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。信息的完整性是信息安全的基本要求。破坏信息的完整性是影响信息安全的常用手段。

二、可用性（availability）

可用性是指信息可被合法用户访问并按要求的特性使用，即当需要时能否存取所需信息。

三、保密性（confidentiality）

保密性是指信息不泄露给非授权的个人和实体，或供其利用的特性。

四、可控性（controllability）

可控性是指对信息的传播及内容具有控制能力。

1．3 信息安全的基本内容

信息安全不能独立于信息系统，其基本内容包括：实体安全，运行安全，信息资产安全和人员安全等几个部分。

1．3．1 实体安全

实体安全就是保护计算机设备、设施以及其它媒体免遭地震、水灾、火灾、有害气体和其它环境事故破坏的措施和过程。它包括三个方面：

环境安全：指对计算机信息系统所在环境的安全保护；

设备安全：指对计算机信息系统设备的安全保护；

媒体安全：指对媒体的安全保护，目的是保护存储在媒体上的信息。其安全功能可归纳为两个方面：一是媒体的防盗；二是媒体的防毁，如防霉和防砸等。

1．3．2 运行安全

运行安全是信息安全的重要环节，是为保障系统功能的安全实现，提供一套安全措施来保护信息处理过程的安全。它包括四个方面：

风险分析：对计算机信息系统进行人工或自动的风险分析。它首先是对系统进行静态的分析（尤其是指系统设计前和系统运行前的风险分析），旨在发现系统的潜在安全隐患；其次是对系统进行动态的分析，即在系统运行过程中测试、跟踪并记录其活动，旨在发现系统运行期的安全漏洞；最后是系统运行后的分析，并提供相应的系统脆弱性分析报告。

审计跟踪：指对计算机系统进行人工或者自动的审计跟踪、保存审计记录和维护详尽的审计日志。其安全功能可归纳为三个方面：记录和跟踪各种系统状态的变化，如提供对系统故意入侵行为的记录和对系统安全功能违反的纪录；实现对各种安全事故的定位，如监控和捕捉各种安全事件；保存、维护和管理审计日志。

备份与恢复：指对系统设备和系统数据的备份与恢复，对系统数据的备份和恢复可以使用多种介质（如磁介质、纸介质、光碟、缩微载体等）。其安全功能可归纳为三个方面：提供场点内高速度、大容量自动的数据存储、备份和

恢复；提供场点外的数据存储、备份和恢复，如通过专用安全记录存储设施对系统内的主要数据进行备份；提供对系统设备的备份。

应急：指在紧急事件或安全事故发生时，保障计算机信息系统继续运行或紧急恢复。其安全功能可归纳为三个方面：紧急事件或安全事故发生时的影响分析；应急计划的概要设计或详细制定；应急计划的测试与完善。

1．3．3 信息资产安全

信息资产包括文件、数据等，其安全是防止信息资产被故意的或偶然的非授权泄漏、更改、破坏或是信息被非法的系统识别和控制，即确保信息的完整性、保密性、可用性和可控性。信息资产安全包括以下七个方面：

操作系统安全：指对计算机信息系统的硬件和软件资源的有效控制，能够为所管理的资源提供相应的安全保护。它们或是以低层操作系统提供的安全机制为基础构造安全模块，或者完全取代底层操作系统，目的是为建立安全信息系统提供一个可信的安全平台；

数据库安全：指对数据库所管理的数据和资源提供安全保护。它一般采用多种安全机制与操作系统相结合，实现数据库的安全保护。一种选择是安全数据库系统，即从系统设计、实现、使用和管理等各个阶段都遵循一套完整的系统安全策略的安全数据库系统。二是以现有数据库系统所提供的功能为基础构造安全模块，旨在增强现有数据库系统的安全性。

网络安全：指提供访问网络资源或使用网络服务的安全保护。网络安全管理是为网络的使用提供安全管理，如帮助协调网络的使用，预防安全事故的发生；跟踪并记录网络的使用，检测系统状态的变化；实现对各种网络安全事故的定位，探测网络安全事件发生的确切位置；提供某种程度的对紧急事件或安全事故的故障排除能力。

病毒防护：指提供对计算机病毒的防护。病毒防护包括单机系统的防护和网络系统的防护。单机系统的防护侧重于保护本地计算机资源，而网络系统的防护侧重于防护网络系统资源。计算机病毒防护产品是通过建立系统保护机制预防、监测和消除病毒。

访问控制：指保证系统的外部用户或内部用户对系统资源的访问以及对敏感信息的访问方式符合组织安全策略。主要包括：出入控制和存取控制。出入控制主要是阻止非授权用户进入机构或组织。一般是以电子技术、生物技术或者电子技术与生物技术结合阻止非授权用户进入。存取控制指主体访问客体时的存取限制，如通过对授权用户存取系统敏感信息时进行安全性检查，以实现对授权用户的存取权限的控制。

加密：即提供数据加密和密钥管理。对数据的加密包括三个方面：对文字

的加密，对语音的加密，对图像、图形的加密。密钥管理包括：密钥的分发或注入，密钥更新，密钥回收，密钥归档，密钥恢复，密钥审计。

鉴别：即提供身份鉴别和信息鉴别。身份鉴别是提供对信息收发方真实身份的鉴别，主要用于阻止非授权用户对系统资源的访问。信息鉴别是提供对信息的正确性、完整性和不可否认性的鉴别。

1．3．4 人员安全

人员安全主要是指信息系统使用人员的安全意识、法律意识、安全技能等。

1．4 本文的主要研究内容：

信息安全涉及的面很广，在本文中，主要探讨了信息安全在公、私两个领域的应用研究。在私人领域，本文研究的是个人隐私权的问题。随着上网人数的增多，网上交易日益频繁，个人在网上的隐私权受到了越来越多的威胁，也引起了更多人的关注。本文从多个方面分析了其内在的原因，并给出了一些解决方法。

在办公领域，本文探讨了电子公文传送中的安全问题。在信息化社会中，政府公文也由原来的文字形式转变为电子文档形式，从而让信息较以往使用纸面数据更加迅速和便利，流传速度更快、更方便。但是，在目前 IP v4 的网络结构下，信息都是毫无保护地在公开的网络上传递。如何能够保证公文不被篡改，如何保证公文的完整性以及如何保证重要的公文不被恶意的网络使用者窃取，这些问题都是本文所希望解决的。

本文对现有的公开密钥体系以及各种加密、解密方法作了介绍与分析，综合了公开加密与传统加密的优点，得到了一种较好的混合式的加密方法。同时，将数字签名技术应用与电子公文传送中，提出了一个解决上述问题的系统，并在 Visual C++的环境中实现了此系统。经过测试，系统能较好地完成各种功能，保证了电子公文在传送中的完整性、保密性以及认证发文单位的正确性。

第二章 密码学的基础知识

在前面一章所介绍的信息安全中，密码学是其中的重要一环，本章将具体介绍密码学中的基本概念和常用术语。

2．1 密码学的基本概念

依据国际标准 ISO/IEC7498-2，密码编码学（cryptography），就是研究对数据进行变换的原理、手段和方法的技术和科学，其目的是掩藏数据的内容，防止对它作了篡改而不被识破或非授权使用。密码分析学（cryptanalytic）是研究密码分析的技术和科学。密码分析（cryptanalysis）就是为了得到秘密信息或包括明文在内的敏感性数据而对密码系统或它的输入输出进行的分析，即对密码原理、手段或方法的攻击。密码编码学和密码分析学两者合并就成为研究密码技术的密码学（cryptology）。

现国际上第一个专门研究密码领域的学会为国际密码研究学会（International Association for Cryptologic Research），简称 IACR。IACR 于 1981 年成立，现每年 5 月于欧洲举办一次学术研讨会，每年 8 月于美国举办学术研讨会，每两年于亚洲举办。

2．2 密码学的常用术语

被伪装的消息称为明文（plaintext）。用某种方法伪装消息以隐藏它的内容的过程称为加密（encryption），被加密的消息称为密文（cipher text），而把密文转变为明文的过程称为解密(decrypt)。加密解密过程如图 2.1 所示。

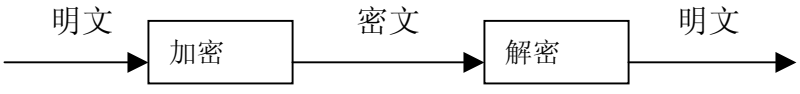


图 2.1 加密和解密

明文一般用 M 或者 P 表示，它可能是位序列、文本文件、位图、数字化的语音序列或数字化的视频图像等等。明文可以被传送或存储，无论在哪种情况，M 指待加密的消息。

密文用 C 表示，它也是二进制数据，有时和 M 一样大，有时稍大。

用来加/解密的数学函数称为密码算法（algorithm）。通常情况下，有两个相关的函数：一个用作加密叫加密算法（encryption algorithm），另一个用作解密叫做解密算法（decryption algorithm）。加密和解密算法的操作通常在一组密钥（key）的控制下进行，分别称为加密密钥（encryption key）和解密密钥（decryption key）。

2．3 密码系统

密码系统是由算法，加上所有可能的明文、密文和密钥组成的。密码系统一般包括以下三个方面：

（1） 用于将明文变换为密文的操作。所有的加密算法基本上都基于置换和替换。置换就是将明文中元素重新排列；替换就是将明文中的每一个元素（位、子介、字符等）映射到另一个元素。最基本的要求是不能丢失信息，即所有的操作都可逆。

（2） 使用大量的密钥。对称密码系统中的加密和解密都使用相同的密钥，非对称密码系统中的加密和解密使用不同的密钥。

（3） 处理明文的方式。分组密码每次将明文块加密成相应的密文快；序列

密码连续地处理明文输入，每次将 1 位明文变换成密文。

一般而言，密码系统依其作用可对信息提供下列功能[2]：

（1） 秘密性（Secrecy or Privacy）:防止非法的接收者发现明文；

（2） 鉴别性（Authenticity）:确定信息来源的合法性，也即此信息确实

是由发送方所传送，而非别人伪造、或利用以前的信息来重叠。

（3） 完整性（Integrity）:确定信息没有被有意或无意地更改，即被部分取代、加入或删除等等。

（4） 不可否认性（Nonrepudiation）:发送方在事后，不可否认其传送过的信息。

传统的密码学往往注重信息的秘密性。但近代密码学认为信息的鉴别性、完整性及不可否认性，在商业上的应用比秘密性更重要。

2．3．1 对称密钥密码系统

在 1976 年以前，也就是在 Diffie 和 Hellman 提出起划时代的论文“New Directions In Cryptography”之前，所谓的密码系统都指的是对称密钥密码

系统。如果加密密钥和解密密钥相同，就称其为对称密码系统（symmetric cryptosystem），也称为单钥密码系统或者私钥密码系统。如果将密钥记作 k,k 可以是众多数值中的任意一个，k 的可能值的范围叫做密钥空间（key space）。加密和解密运算都使用这个密钥，即运算都依赖于密钥，于是加密解密函数可表示成：

$E_K(M)=C$

$D_K(C)=M$

并且加密解密函数具有如下特性:

$D_K(E_K(M))=M$ （如图 2.2 所示）

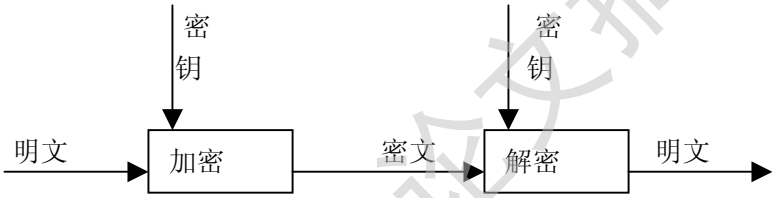


图 2.2 对称密码系统

一个安全的对称密钥密码系统，可以达到下列功能：

1. 保护信息机密：明文经加密后，除非拥有解密密钥，外人无从了解其内容；
2. 认证发送方之身份：接收方任意选择一随机数 r,请发送方加密成密文 C，送回给接收方。接收方再将 C 解密，若能还原成原来的 r,则可确认发送方的身份无误，否则则是第三者冒充。因为只有发送方和接收方知道加密密钥,因此只有他能将此随机数 r 所对应的密文 C 求出，其他人因为不知道加密密钥，因而无法求出正确的 C。这种认证发送方身份的方法，还广泛使用于银行体系中。
3. 确保信息完整性：在许多不需要隐藏信息内容，但需要确保信息内容不被更改的场合中，发送方可将明文加密后的密文附加于明文之后传送给接收方，接收方可将附加的密文解密或者将明文加密，来对照二者是否相符。若相符则表示明文为正确，否则可能被改动。

但是，对称密钥密码系统具有下列缺点：

1. 密钥分配问题难以解决，在发送方和接收方之间必须设立一秘密通道来安全地传送密钥；
2. 密钥的数目太大，若网络中有 n 人，则每一人必须拥有 n-1 把密钥，网络中共需有 n（n-1）/2 把不同的密钥；
3. 无法达到不可否认服务：由于发送方和接收方都知道对方的密钥，因此发送方可以在事后否认他先前送过的任何信息。因为接收方可以任意地

伪造或篡改，而第三方并无法分辨是发送方抵赖曾经送过信息，还是接收方自己捏造的。

由于对称密码系统存在这样的缺点，1976 年诞生了公开密钥密码系统。

2．3．2 公开密钥密码系统

非对称密码系统又称为公开密码系统，其提出的目的是为了解决利用传统密码体制进行密钥分发时遇到的两个难题：一是密钥分发。在利用传统密码进行密钥分发时，可以有两种选择，一是已经共享一对密钥，通过某种方式写给用户的；二是利用一个密钥分发中心，而密钥分发中心与密码学的本质相违背：即能维持通信中的整体保密。第二个难题就是本论文所讨论的问题：数字签名。人们需要设计出一种强有力的方法，使得能在许多用户之中，准确地找出是由哪一方发送的消息。

Diffie 和 Hellman 在 1976 年设计出一种方法，取得了理论上的突破，同时解决了这两个问题，而且与使用了四千年的传统方法有了巨大的差异，即公开密钥密码体制。

如果加密密钥和解密密钥不相同，则称其为非对称密码系统（asymmetric cryptosystem），也称为双钥密码系统或公开密钥密码系统。如果将加密密钥记作 K1，相应的解密密钥记作 K2，在这种情况下加密解密函数可表示成：

$$E_{K1}(M)=C$$

$$D_{K2}(C)=M$$

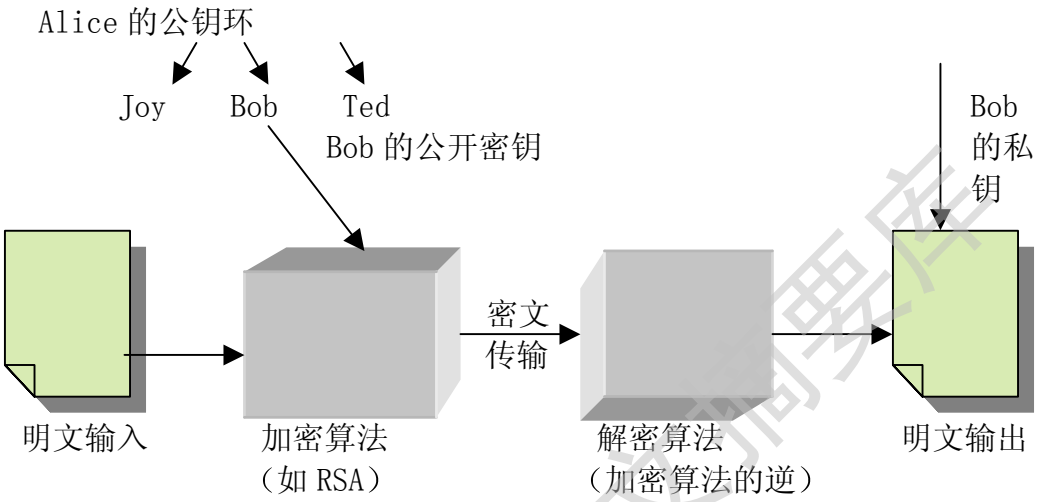
公开密钥算法使用一个密钥进行加密，同时使用一个相关的不同密钥用于解密，其算法具有以下特征：

1．如果仅仅知道密码算法和加密密钥的知识，要确定解密密钥在计算上是不可行的。

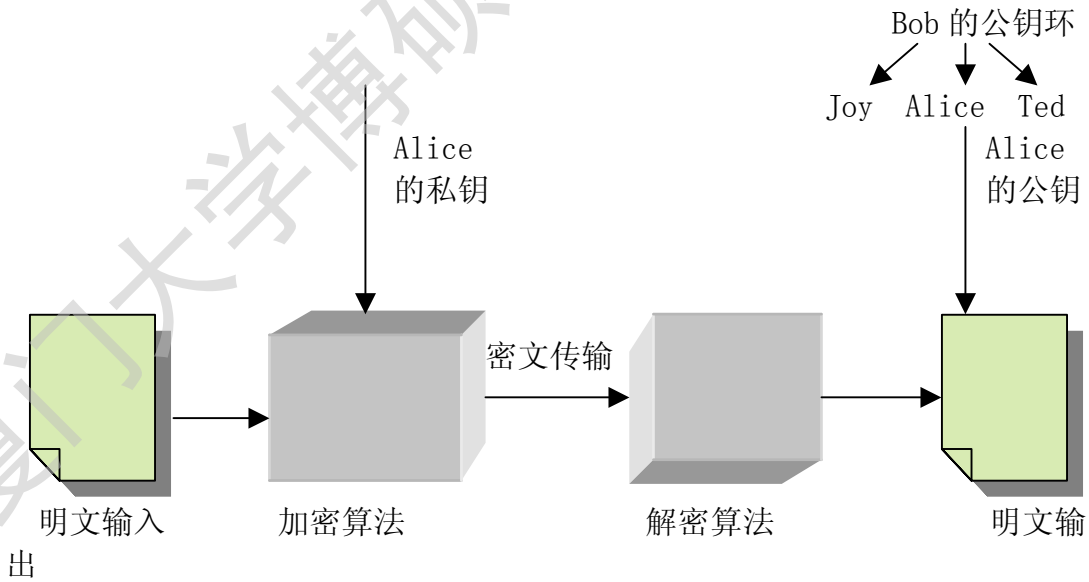
如果是 RSA 算法，还应有如下的特征：

2．两个相关的密钥都可用于加密，而另一个则可用于解密。

公开密钥算法的加密过程如图 2.3 所示：



（a）加密、解密过程



（b）鉴别过程

图 2.3 公开密钥算法的加密、解密及鉴别过程

其主要的步骤如下：

1．网络中的每个端系统都要生成一对密钥，用于对系统收到的消息进行加/解密；
2．每一个系统都将它的加密密钥放入一个公开的登记处或文件中，这个密钥就是公开密钥，相应私钥被私下保存；
3．如果 A 希望向 B 发送一个消息，他将使用 B 的公开密钥对消息加密；
4．当 B 收到消息时，B 用他的私钥解密，没有其他的用户在收到该消息后能解开它，因为只有 B 才知道 B 的密钥。

在这种方法中，所有的参与者都能访问公开密钥，私有密钥在本地由参与者局部生成，不需要传送，只要系统对其私钥完全控制，则进入的通信是安全的。任何时候，系统都可以改变他的私有密钥并将相应的公开密钥公之于众，替代原来的公钥。下表总结了传统密钥和公开密钥加密的一些重要指标，为了便于区别，一般称传统加密中的密钥为秘密密钥，在公开加密中使用的两个密钥分别称为公开密钥和私有密钥。

表 2.1 传统密钥加密和公开密钥加密

传统密钥加密	公开密钥加密
工作需要 1、使用相同密钥的相同算法用于加密/解密； 2、发送者和接收者必须共享相同算法和密钥	工作需要 1、使用一对密钥的加密和解密算法，其中一个密钥用于加密，一个用于解密； 2、发送者和接收者必须有一对匹配的密钥
安全需求 1、密钥必须秘密保存； 2、如果没有其它消息可用，解密消息是不可能的，至少是不实际的； 3、当知道算法和密文样本时，一定没有有效的方法确定密钥。	安全需求 1、两个密钥中的一个必须保密； 2、如果没有其它信息可用，则解密消息是不可能的，至少是不实际的； 3、如果已知算法和密钥，并有充分的密文消息，一定没有有效的方法确定密钥。

一般而言，公开密钥密码体制可以用于以下三个范畴：
1．加密/解密：发送者利用接收者的公开密钥加密消息；
2．数字签名：发送者使用自己的私钥对消息进行“签名”。其方式是将密码算法应用于消息或者由消息的一个函数得到的一小块数据上而达到签名的目的；
3．密钥交换：通信双方协作以交换会话密钥，有多种可能的方法，这些

方法涉及一方或双方的密钥。

常用的公开密钥加密算法有很多，有些适宜于以上三种，有的只能满足以上一种或两种目的。表 2.2 描述了各种算法支持的应用情况：

表 2.2 公开密钥体制应用

算法	加密/解密	数字签名	密钥交换
RSA	能	能	能
Diffie-Hellman	不能	不能	能
DSS	不能	能	能

2．4 数字签名

前一章所提出的问题中，公文的完整性和发文单位的认证，都可以用数字签名的技术来解决。数字签名技术是公开密钥体制的一种应用，于 1976 年由 Diffle 和 Hellman 提出，随后在学术界尤其是计算机网络界引起了广泛的重视。特别是随着 Internet 飞速发展和广泛应用，人们对信息安全的要求越来越高，数字签名技术获得了更多的研究和应用。

数字签名的运作方式如图 2.4 所示，发送端（Alice）在签署文件之前，先对其要签署的文件，利用一个单项散列函数，产生一个用来区别文件的单项散列函数值，再由发送端使用其所拥有的密钥，对这一函数值，执行一个签名的运算，产生一个数字签名，再将此签名及文件一并送交给接收者。

接收端（Bob）收到文件和签名后，可以验证发送端所送来的签名，以断定文件的真伪，确定是否是发送端所发送的。首先，接收端使用发送端的公钥，对发送端利用其密钥所签署的签名解密。接收端再利用与发送端相同的单向散列函数，针对此份文件，产生它的散列函数值，并将此值与先前解密结果比较。若比较结果相同，则可证明这一签名确实由发送端发出，若不相同则拒绝此签名，其错误原因可能是网络传输过程中有错误发生或有人恶意欺骗。